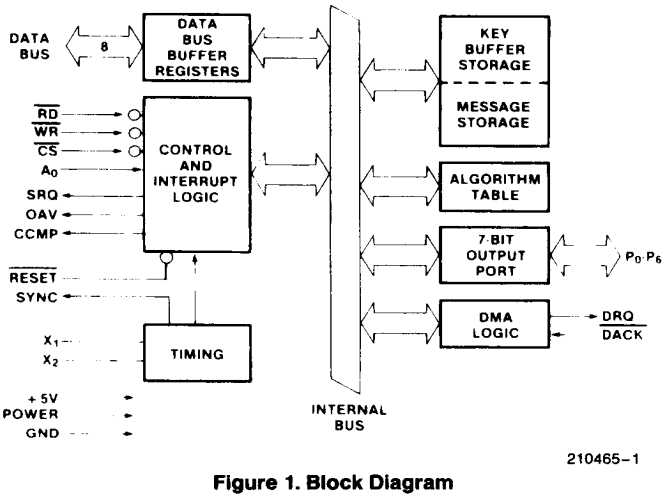
8294A
DATA ENCRYPTION/DECRYPTION UNIT

- **Certified by National Bureau of Standards**
- **400 Byte/Sec Data Conversion Rate**
- **64-Bit Data Encryption Using 56-Bit Key**
- **DMA Interface**
- **3 Interrupt Outputs to Aid in Loading and Unloading Data**
- **7-Bit User Output Port**
- **Single 5V ± 10% Power Supply**
- **Fully Compatible with iAPX-86, 88, MCS-85™, MCS-80™, MCS-51™, and MCS-48™ Processors**
- **Implements Federal Information Processing Data Encryption Standard**
- **Encrypt and Decrypt Modes Available**

The Intel® 8294A Data Encryption Unit (DEU) is a microprocessor peripheral device designed to encrypt and decrypt 64-bit blocks of data using the algorithm specified in the Federal Information Processing Data Encryption Standard. The DEU operates on 64-bit text words using a 56-bit user-specified key to produce 64-bit cipher words. The operation is reversible: if the cipher word is operated upon, the original text word is produced. The algorithm itself is permanently contained in the 8294A; however, the 56-bit key is user-defined and may be changed at any time.

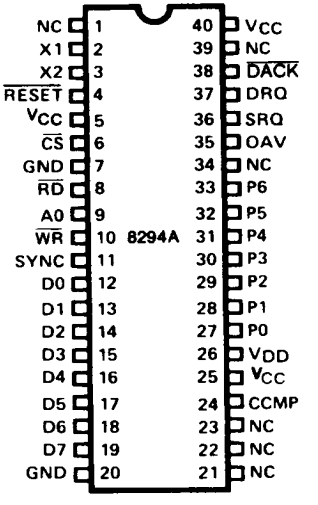
The 56-bit key and 64-bit message data are transferred to and from the 8294A in 8-bit bytes by way of the system data bus. A DMA interface and three interrupt outputs are available to minimize software overhead associated with data transfer. Also, by using the DMA interface two or more DEUs may be operated in parallel to achieve effective system conversion rates which are virtually any multiple of 400 bytes/second. The 8294A also has a 7-bit TTL compatible output port for user-specified functions.

Because the 8294A implements the NBS encryption algorithm it can be used in a variety of Electronic Funds Transfer applications as well as other electronic banking and data handling applications where data must be encrypted.



210465-1

Figure 1. Block Diagram



210465-2

Figure 2. Pin Configuration

November 1986
Order Number: 210465-004

Table 1. Pin Description

Symbol	Pin No.	Type	Name and Function
NC	1		**NO CONNECTION.**
X1 X2	2 3		**CRYSTAL:** Inputs for crystal, L-C or external timing signal to determine internal oscillator frequency.
$\overline{RESET}$	4	I	**RESET:** A low signal to this pin resets the 8294A.
V_{CC}	5		**POWER:** Tied high.
$\overline{CS}$	6	I	**CHIP SELECT:** A low signal to this pin enables reading and writing to the 8294A.
GND	7		**GROUND:** This pin must be tied to ground.
$\overline{RD}$	8	I	**READ:** An active low read strobe at this pin enables the CPU to read data and status from the internal DEU registers.
A_0	9	I	**ADDRESS:** Address input used by the CPU to select DEU registers during read and write operations.
$\overline{WR}$	10	I	**WRITE:** An active low write strobe at this pin enables the CPU to send data and commands to the DEU.
SYNC	11	O	**SYNC:** High frequency (Clock ÷ 15) output. Can be used as a strobe for external circuitry.
D_0 D_1 D_2 D_3 D_4 D_5 D_6 D_7	12 13 14 15 16 17 18 19	I/O	**DATA BUS:** Three-state, bi-directional data bus lines used to transfer data between the CPU and the 8294A.
GND	20		**GROUND:** This pin must be tied to ground.
V_{CC}	40		**POWER:** +5V power input: +5V ±10%.
NC	39		**NO CONNECTION.**
$\overline{DACK}$	38	I	**DMA ACKNOWLEDGE:** Input signal from the 8257 DMA Controller acknowledging that the requested DMA cycle has been granted.
DRQ	37	O	**DMA REQUEST:** Output signal to the 8257 DMA Controller requesting a DMA cycle.
SRQ	36	O	**SERVICE REQUEST:** Interrupt to the CPU indicating that the 8294A is awaiting data or commands at the input buffer. SRQ = 1 implies IBF = 0.
OAV	35	O	**OUTPUT AVAILABLE:** Interrupt to the CPU indicating that the 8294A has data or status available in its output buffer, OAV = 1 implies OBF = 1.
NC	34		**NO CONNECTION.**

Table 1. Pin Description (Continued)

Symbol	Pin No.	Type	Name and Function
P6 P5 P4 P3 P2 P1 P0	33 32 31 30 29 28 27	O	**OUTPUT PORT:** User output port lines. Output lines available to the user via a CPU command which can asset selected port lines. These lines have nothing to do with the encryption function. At power-on, each line is in a 1 state.
V_{DD}	26		**POWER:** +5V power input. (+5V ±10%) Low power standby pin.
V_{CC}	25		**POWER:** Tied high.
CCMP	24	O	**CONVERSION COMPLETE:** Interrupt to the CPU indicating that the encryption/decryption of an 8-byte block is complete.
NC	23		**NO CONNECTION.**
NC	22		**NO CONNECTION.**
NC	21		**NO CONNECTION.**

FUNCTIONAL DESCRIPTION

OPERATION

The data conversion sequence is as follows:

1) A Set Mode command is given, enabling the desired interrupt outputs.
2) An Enter New Key command is issued, followed by 8 data inputs which are retained by the DEU for encryption/decryption. Each byte must have odd parity.
3) An Encrypt Data or Decrypt Data command sets the DEU in the desired mode.

After this, data conversions are made by writing 8 data bytes and then reading back 8 converted data bytes. Any of the above commands may be issued between data conversions to change the basic operation of the DEU; e.g., a Decrypt Data command could be issued to change the DEU from encrypt mode to decrypt mode without changing either the key or the interrupt outputs enabled.

INTERNAL DEU REGISTERS

Four internal registers are addressable by the master processor: 2 for input, and 2 for output. The following table describes how these registers are accessed.

$\overline{RD}$	$\overline{WR}$	$\overline{CS}$	A_0	Register
1	0	0	0	Data Input Buffer
0	1	0	0	Data Output Buffer
1	0	0	1	Command Input Buffer
0	1	0	1	Status Output Buffer
X	X	1	X	Don't Care

The functions of each of these registers are described below.

Data Input Buffer—Data written to this register is interpreted in one of three ways, depending on the preceding command sequence.

1) Part of a key.
2) Data to be encrypted or decrypted.
3) A DMA block count.

Data Output Buffer—Data read from this register is the output of the encryption/decryption operation.

Command Input Buffer—Commands to the DEU are written into this register. (See command summary below.)

Status Output Buffer—DEU status is available in this register at all times. It is used by the processor for poll-driven command and data transfer operations.

STATUS BIT:	7	6	5	4	3	2	1	0
FUNCTION:	X	X	X	KPE	CF	DEC	IBF	OBF

OBF Output Buffer Full; OBF = 1 indicates that output from the encryption/decryption function is available in the Data Output Buffer. It is reset when the data is read.

IBF Input Buffer Full; A write to the Data Input Buffer or to the Command Input Buffer sets IBF = 1. The DEU resets this flag when it has accepted the input byte. Nothing should be written when IBF = 1.

DEC Decrypt; indicates whether the DEU is in an encrypt or a decrypt mode. DEC = 1 implies the decrypt mode. DEC = 0 implies the encrypt mode.

After 8294A has accepted a 'Decrypt Data' or 'Encrypt Data' command, 11 cycles are required to update the DEC bit.

CF Completion Flag; This flag may be used to indicate any or all of three events in the data transfer protocol.

1) It may be used in lieu of a counter in the processor routine to flag the end of an 8-byte transfer.
2) It must be used to indicate the validity of the KPE flag.
3) It may be used in lieu of the CCMP interrupt to indicate the completion of a DMA operation.

KPE Key Parity Error; After a new key has been entered, the DEU uses this flag in conjunction with the CF flag to indicate correct or incorrect parity.

COMMAND SUMMARY

1 — Enter New Key

OP CODE:	0	1	0	0	0	0	0	0
	MSB							LSB

This command is followed by 8 data byte inputs which are retained in the key buffer (RAM) to be used in encrypting and decrypting data. These data bytes must have odd parity represented by the LSB.

2 — Encrypt Data

OP CODE:	0	0	1	1	0	0	0	0
	MSB							LSB

This command puts the 8294A into the encrypt mode.

3 — Decrypt Data

OP CODE:	0	0	1	0	0	0	0	0
	MSB							LSB

This command puts the 8294A into the decrypt mode.

4 — Set Mode

OP CODE:	0	0	0	0	A	B	C	D
	MSB							LSB

where:

A is the OAV (Output Available) interrupt enable
B is the SRQ (Service Request) interrupt enable
C is the DMA (Direct Memory Access) transfer enable
D is the CCMP (Conversion Complete) interrupt enable

This command determines which interrupt outputs will be enabled. A "1" in bits A, B, or D will enable the OAV, SRQ, or CCMP interrupts respectively. A "1" in bit C will allow DMA transfers. When bit C is set the OAV and SRQ interrupts should also be enabled (bits A, B = 1). Following the command in which bit C, the DMA bit, is set, the 8294 will expect one data byte to specify the number of 8-byte blocks to be converted using DMA.

5 — Write to Output Port

OP CODE:	1	P_6	P_5	P_4	P_3	P_2	P_1	P_0
	MSB							LSB

This command causes the 7 least significant bits of the command byte to be latched as output data on the 8294 output port. The initial output is 1111111. Use of this port is independent of the encryption/decryption function.

PROCESSOR/DEU INTERFACE PROTOCOL

ENTERING A NEW KEY

The timing sequence for entering a new key is shown in Figure 3. A flowchart showing the CPU software to accommodate this sequence is given in Figure 4.

After the Enter New Key command is issued, 8 data bytes representing the new key are written to the data input buffer (most significant byte first). After the eighth byte is entered into the DEU, CF goes true (CF = 1). The CF bit goes false again when KPE is valid. The CPU can then check the KPE flag. If KPE = 1, a parity error has been detected and the DEU has not accepted the key. Each byte is checked for odd parity, where the parity bit is the LSB of each byte.

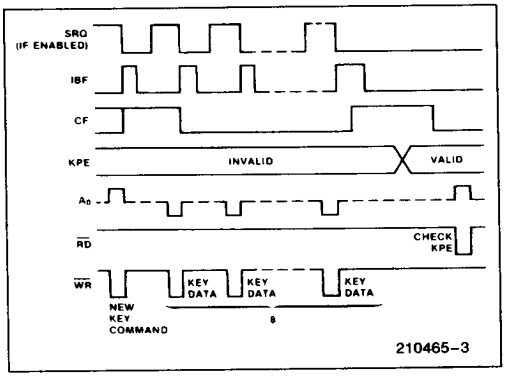


Figure 3. Entering a New Key

Since CF = 1 only for a short period of time after the last byte is accepted, the CPU which polls the CF flag might miss detecting CF = 1 momentarily. Thus, a counter should be used, as in Figure 4, to flag the end of the new key entry. Then CF is used to indicate a valid KPE flag.

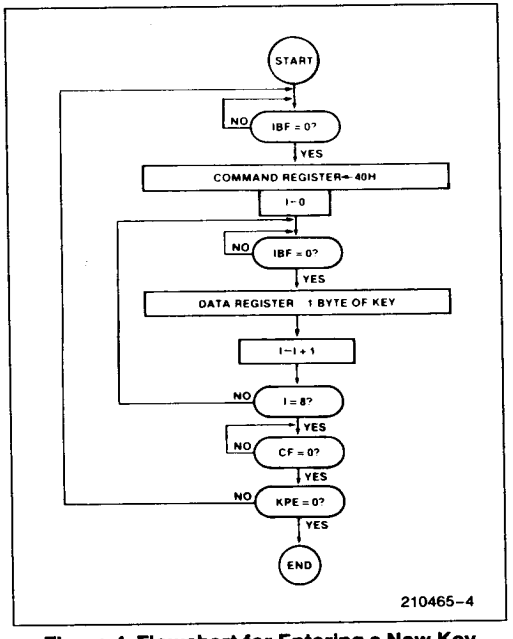


Figure 4. Flowchart for Entering a New Key

ENCRYPTING OR DECRYPTING DATA

Figure 5 shows the timing sequence for encrypting or decrypting data. The CPU writes 8 data bytes to the DEU's data input buffer for encryption/decryption. CF then goes true (CF = 1) to indicate that the DEU has accepted the 8-byte block. Thus, the CPU may test for IBF = 0 and CF = 1 to terminate the input mode, or it may use a software counter. When the encryption/decryption is complete, the CCMP and OAV interrupts are asserted and the OBF flag is set true (OBF = 1). OAV and OBF are set false again after each of the converted data bytes is read back by the CPU. The CCMP interrupt is set false, and remains false, after the first read. After 8 bytes have been read back by the CPU, CF goes false (CF = 0). Thus, the CPU may test for CF = 0 to terminate the read mode. Also, the CCMP interrupt may be used to initiate a service routine which performs the next series of 8 data reads and 8 data writes.

Figure 6 offers two flowcharts outlining the alternative means of implementing the data conversion protocol. Either the CF flag or a software counter may be used to end the read and write modes.

SRQ = 1 implies IBF = 0, OAV = 1 implies OBF = 1. This allows interrupt routines to do data transfers without checking status first. However, the OAV service routine must detect and flag the end of a data conversion.

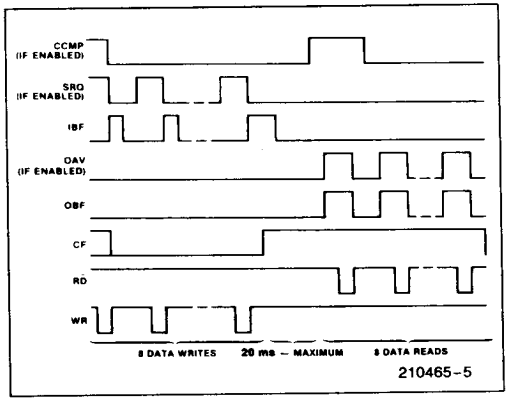
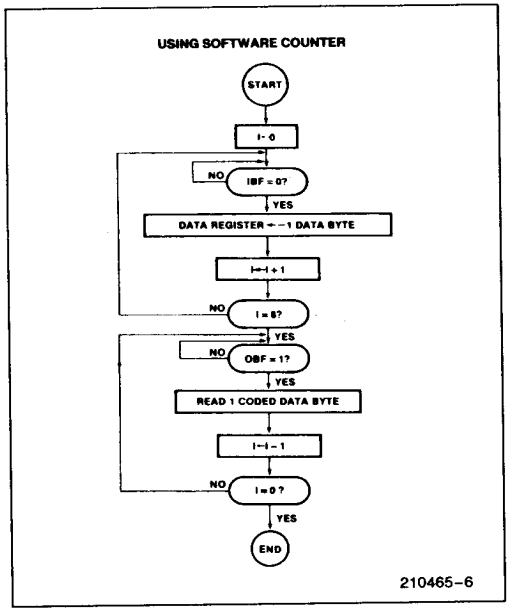


Figure 5. Encrypting/Decrypting Data



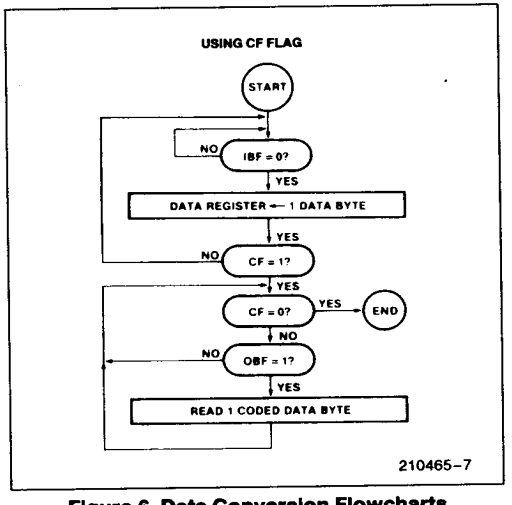


Figure 6. Data Conversion Flowcharts

USING DMA

The timing sequence for data conversions using DMA is shown in Figure 7. This sequence can be better understood when considered in conjunction with the hardware DMA interface in Figure 8. Note

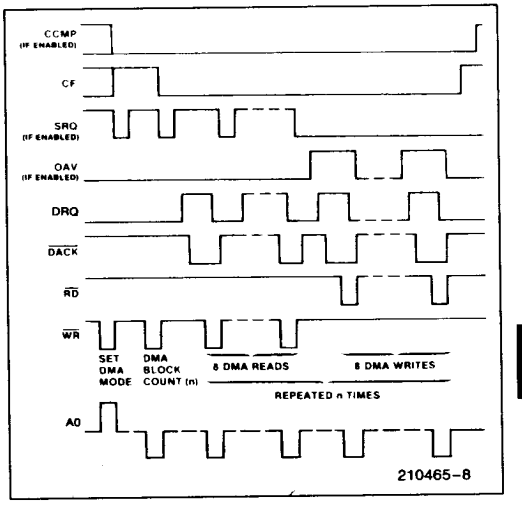


Figure 7. DMA Sequence

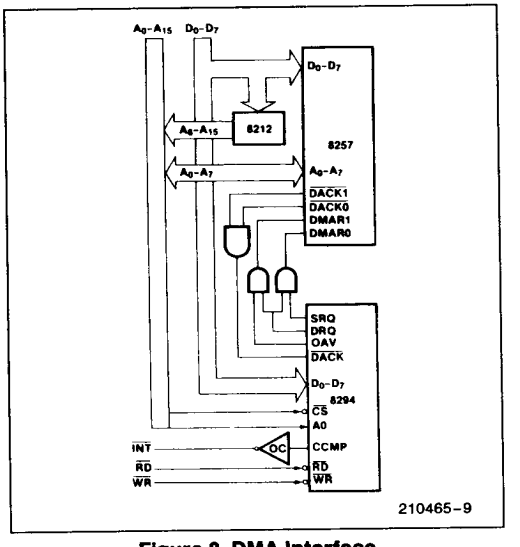


Figure 8. DMA Interface

that the use of the DMA feature requires 3 external AND gates and 2 DMA channels (one for input, one for output). Since the DEU has only one DMA request pin, the SRQ and OAV outputs are used in conjunction with two of the AND gates to create separate DMA request outputs for the 2 DMA channels. The third AND gate combines the two active-low $\overline{DACK}$ inputs.

To initiate a DMA transfer, the CPU must first initialize the two DMA channels as shown in the flowchart in Figure 9. It must then issue a Set Mode command to the DEU enabling the OAV, SRQ, and DMA outputs. The CCMP interrupt may be enabled or disabled, depending on whether that output is desired. Following the Set Mode command, there must be a data byte giving the number of 8-byte blocks of data ($n < 256$) to be converted. The DEU then generates the required number of DMA requests to the 2 DMA channels with no further CPU intervention. When the requested number of blocks has been converted, the DEU will set CF and assert the CCMP interrupt (if enabled). CCMP then goes false again with the next write to the DEU (command or data). Upon completion of the conversion, the DMA mode is disabled and the DEU returns to the encrypt/decrypt mode. The enabled interrupt outputs, however, will remain enabled until another Set Mode command is issued.

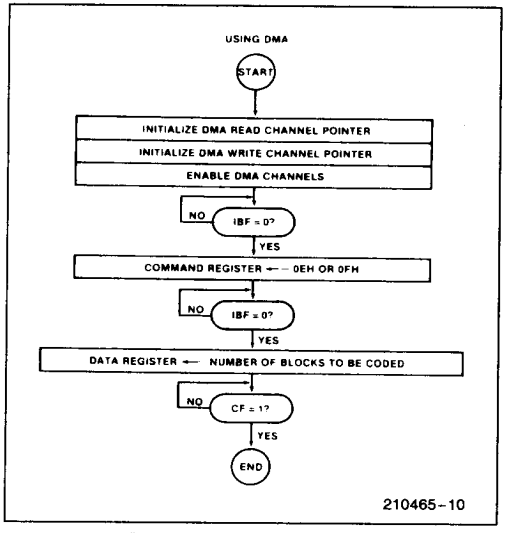


Figure 9. DMA Flowchart

SINGLE BYTE COMMANDS

Figure 10 shows the timing and protocol for single byte commands. Note that any of the commands is effective as a pacify command in that they may be entered at any time, expect during a DMA conversion. The DEU is thus set to a known state. However, if a command is issued out of sequence, an additional protocol is required (Figure 11). The CPU must wait until the command is accepted (IBF = 0). A data read must then be issued to clear anything the preceding command sequence may have left in the Data Output Buffer.

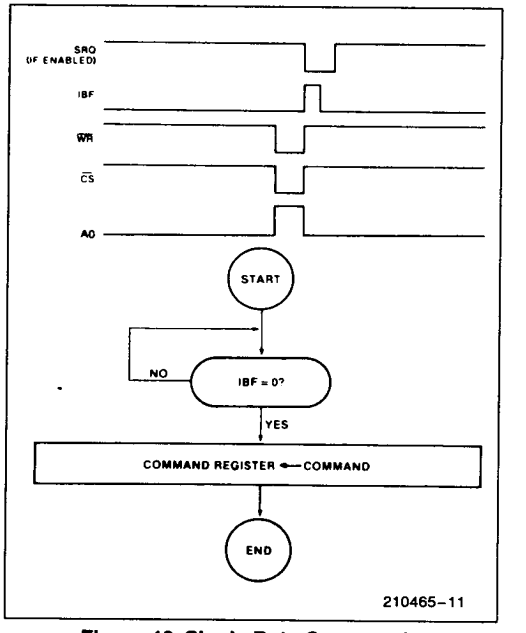


Figure 10. Single Byte Commands

CPU/DEU INTERFACES

Figures 12 through 15 illustrate four interface configurations used in the CPU/DEU data transfers. In all cases SRQ will be true (if enabled) and IBF will be false when the DEU is ready to accept data or commands.

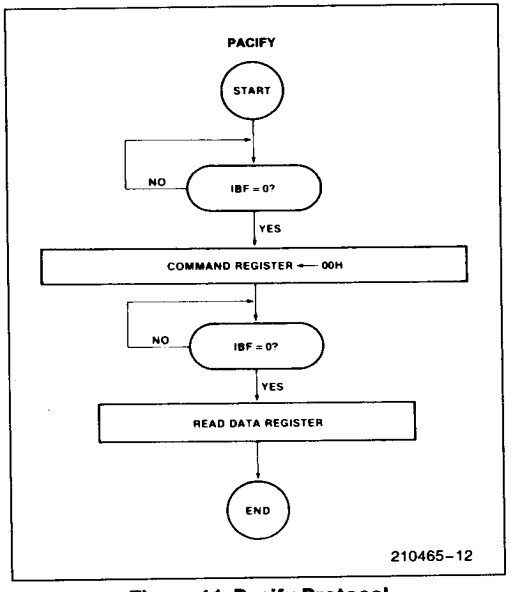


Figure 11. Pacify Protocol

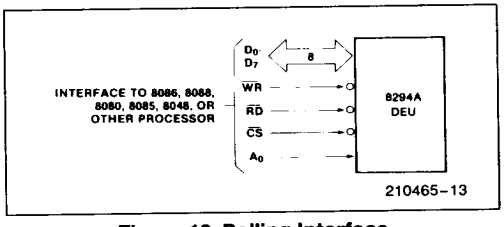


Figure 12. Polling Interface

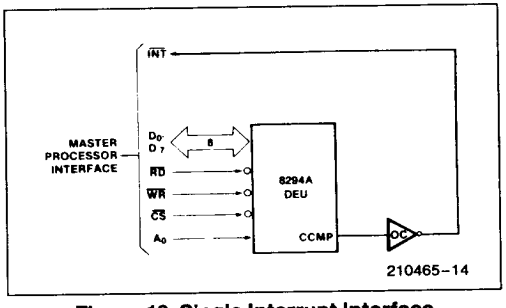


Figure 13. Single Interrupt Interface

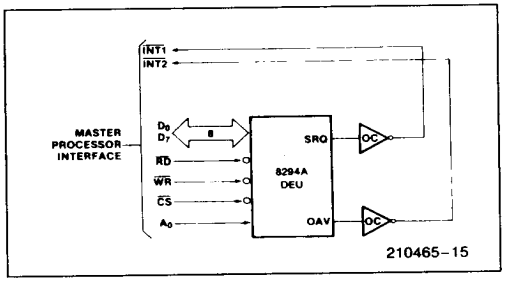


Figure 14. Dual Interrupt Interface

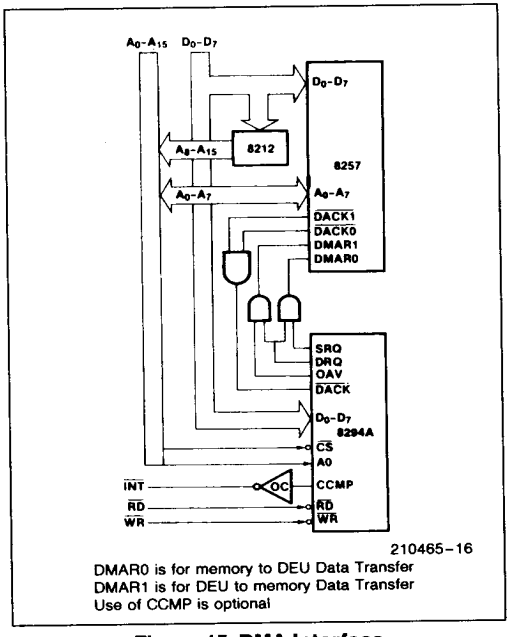


Figure 15. DMA Interface

OSCILLATING AND TIMING CIRCUITS

The 8294A's internal timing generation is controlled by a self-contained oscillator and timing circuit. A choice of crystal, L-C or external clock can be used to derive the basic oscillator frequency.

The resident timing circuit consists of an oscillator, a state counter and a cycle counter as illustrated in Figure 16.

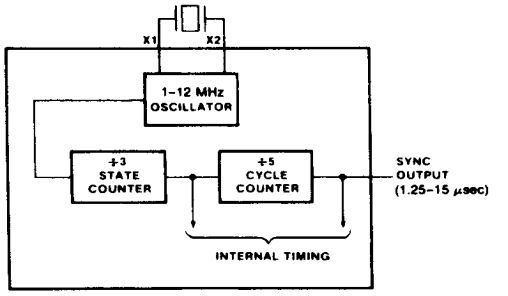
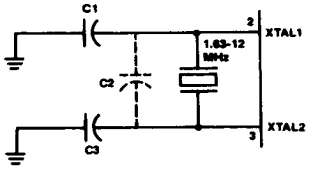


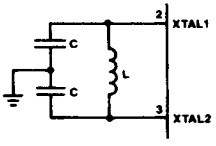
Figure 16. Oscillator Configuration

OSCILLATOR MODE



C1 = 5 pF
C2 = Crystal + Stray < 15 pF
C3 = 20–30 pF
Crystal series resistance should be less than 75Ω at 6 MHz; less than 180Ω at 3.6 MHz; less than 30Ω at 12 MHz.

LC OSCILLATOR MODE



$$1 = \frac{1}{2\pi\sqrt{LC'}}$$

$$C' = \frac{C + 3\,C_{PP}}{2}$$

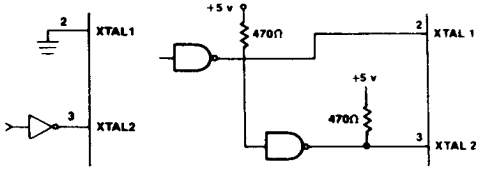
C_{PP} = 5–10 pF Pin-to-Pin Capacitance

L	C	Nominal
9 μH	20 pF	11.5 MHz
45 μH	20 pF	5.2 MHz
120 μM	20 pF	3.2 MHz

Each C should be approximately 20 pF including stray capacitance.

Figure 17. Recommended Crystal

DRIVING FROM EXTERNAL SOURCE—TWO OPTIONS



For the 8294A XTAL2 must be high 35–65% of the period.
Rise and fall times must not exceed 10 ns.
Resistor to V_{CC} is needed to ensure V_{IH} = 3.0V if TTL circuitry is used.

Figure 18. Recommended Connection for External Clock Signal

ABSOLUTE MAXIMUM RATINGS*

Ambient Temperature Under Bias . . . . 0°C to +70°C
Storage Temperature . . . . . −65°C to +150°C
Voltage on Any Pin With Respect to Ground . . . . . −0.5V to +7V
Power Dissipation . . . . . 1.5 Watt

NOTICE: This is a production data sheet. The specifications are subject to change without notice.

**WARNING: Stressing the device beyond the "Absolute Maximum Ratings" may cause permanent damage. These are stress ratings only. Operation beyond the "Operating Conditions" is not recommended and extended exposure beyond the "Operating Conditions" may affect device reliability.*

D.C. AND OPERATING CHARACTERISTICS

T_A = 0°C to +70°C, V_{CC} = +5V ±10%, V_{SS} = 0V

Symbol	Parameter	Limits			Unit	Test Conditions
		Min	Typ	Max		
V_{IL}	Input Low Voltage (All Except X_1, X_2, RESET)	−0.5		0.8	V	
V_{IL1}	Input Low Voltage (X_1, X_2, RESET	−0.5		0.6	V	
V_{IH}	Input High Voltage (All Except X_1, RESET)	2.0		V_{CC}	V	
V_{IH1}	Input High Voltage (X_1, RESET	3.5		V_{CC}	V	
V_{IH2}	Input High Voltage (X_2)	2.2		V_{CC}	V	
V_{OL}	Output Low Voltage (D_0–D_7)			0.45	V	I_{OL} = 2.0 mA
V_{OL1}	Output Low Voltage (All Other Outputs)			0.45	V	I_{OL} = 1.6 mA
V_{OH}	Output High Voltage (D_0–D_7)	2.4			V	I_{OH} = −400 μA
V_{OH1}	Output High Voltage (All Other Outputs)	2.4			V	I_{OH} = −50 μA
I_{IL}	Input Leakage Current (RD, WR, CS, A_0)			±10	μA	$V_{SS} \le V_{IN} \le V_{CC}$
I_{OFL}	Output Leakage Current (D_0–D_7, High Z State)			±10	μA	V_{SS} + 0.45 ≤ $V_{OUT} \le V_{CC}$
I_{DD}	V_{DD} Supply Current		5	20	mA	
$I_{DD} + I_{CC}$	Total Supply Current		60	135	mA	
I_{LI}	Low Input Load Current (Pins 24, 27–38)			0.3	mA	V_{IL} = 0.8V
I_{LI1}	Low Input Load Current (RESET)			0.2	mA	V_{IL} = 0.8V
I_{IH}	Input High Leakage Current (Pins 24, 27–38)			100	μA	$V_{IN} = V_{CC}$
C_{IN}	Input Capacitance			10	pF	
$C_{I/O}$	I/O Capacitance			20	pF	

3

A.C. CHARACTERISTICS $T_A = 0°C$ to $+70°C$, $V_{CC} = V_{DD} = +5V \pm 10\%$, $V_{SS} = 0V$

DBB READ

Symbol	Parameter	Min	Max	Unit	Test Conditions
t_{AR}	$\overline{CS}$, A_0 Setup to $\overline{RD}\downarrow$	0		ns	
t_{RA}	$\overline{CS}$, A_0 Hold After $\overline{RD}\uparrow$	0		ns	
t_{RR}	$\overline{RD}$ Pulse Width	160		ns	
t_{AD}	$\overline{CS}$, A_0 to Data Out Delay		130	ns	$C_L = 100$ pF
t_{RD}	$\overline{RD}\downarrow$ to Data Out Delay		130	ns	$C_L = 100$ pF
t_{DF}	$\overline{RD}\uparrow$ to Data Float Delay		85	ns	
t_{CY}	Cycle Time	1.25	15	μs	1–12 MHz Crystal

DBB WRITE

Symbol	Parameter	Min	Max	Unit	Test Conditions
t_{AW}	$\overline{CS}$, A_0 Setup to $\overline{WR}\downarrow$	0		ns	
t_{WA}	$\overline{CS}$, A_0 Hold After $\overline{WR}\uparrow$	0		ns	
t_{WW}	$\overline{WR}$ Pulse Width	160		ns	
t_{DW}	Data Setup to $\overline{WR}\uparrow$	130		ns	
t_{WD}	Data Hold to $\overline{WR}\uparrow$	0		ns	

DMA AND INTERRUPT TIMING

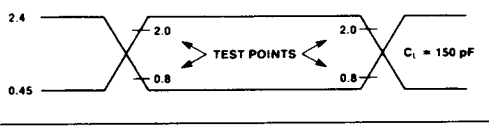
Symbol	Parameter	Min	Max	Unit	Test Conditions
t_{ACC}	$\overline{DACK}$ Setup to Control	0		ns	
t_{CAC}	$\overline{DACK}$ Hold After Control	0		ns	
t_{ACD}	$\overline{DACK}$ to Data Valid		130	ns	$C_L = 100$ pF
t_{CRQ}	Control L.E. to DRQ T.E.		110	ns	
t_{CI}	Control T.E. to Interrupt T.E.		400	ns	

CLOCK

Symbol	Parameter	Min	Max	Units
t_{CY}	Cycle Time	1.25	9.20	μs(1)
t_{CYC}	Clock Period	83.3	613	ns
t_{PWH}	Clock High Time	38		ns
t_{PWL}	Clock Low Time	38		ns
t_R	Clock Rise Time		10	ns
t_F	Clock Fall Time		10	ns

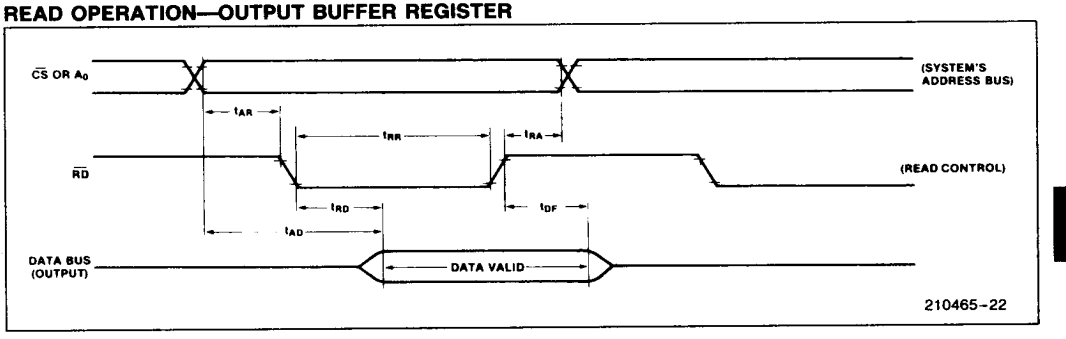
NOTE:
1. $t_{CY} = 15/f(XTAL)$

A.C. TESTING INPUT, OUTPUT WAVEFORM

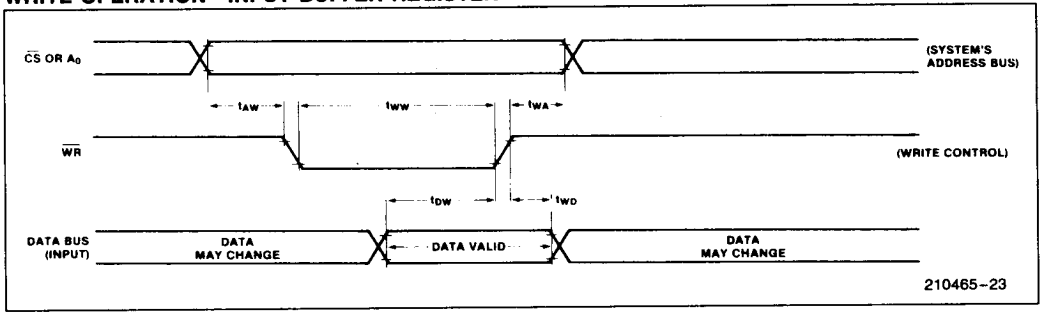


WAVEFORMS

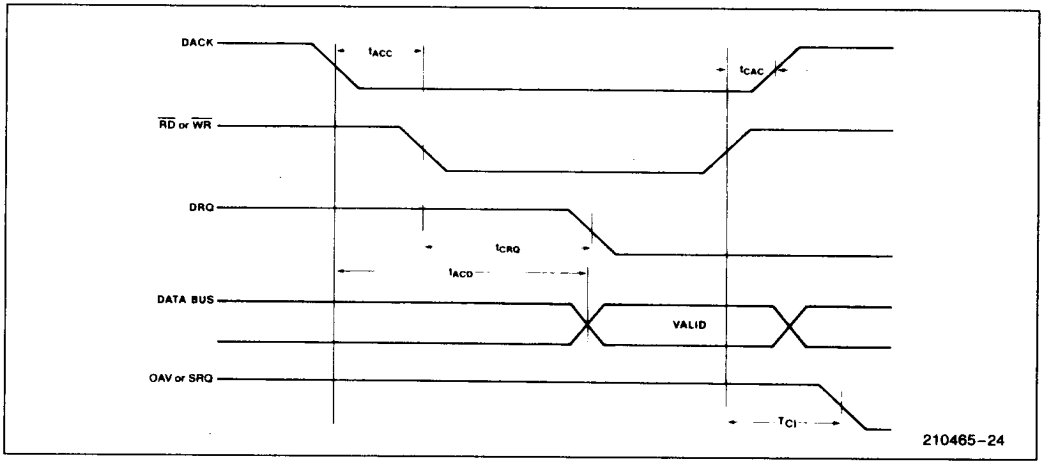
READ OPERATION—OUTPUT BUFFER REGISTER



WRITE OPERATION—INPUT BUFFER REGISTER



DMA AND INTERRUPT TIMING



CLOCK TIMING